UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,548	08/29/2000	Barry Atkins	RPS920000026US1	9903

7590 04/07/2004

BRACEWELL & PATTERSON, L.L.P.
Intellectual Property Law
P.O. Box 969
Austin, TX 78767-0969

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2132	8

DATE MAILED: 04/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/651,548	Applicant(s) ATKINS ET AL.	
	Examiner Kyung H Shin	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 August 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 August 2000* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2,6*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application papers dated 8/29/2000.

2. Claims **1-24** are pending. Claims **1, 9,** and **17** are **independent**.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1- 24** are rejected under 35 U.S.C. 102(e) as being unpatentable over **Challener et al.** (U.S. Patent No. 6,704,868 B1: Methods for Associating for a Pass Phase with a Secured Public/Private Key Pair, File date - Nov. 12, 1999).

Regarding Claim 1, 9, 17, Challener discloses a method, a system and program product for managing a user key used to sign a message for a data processing system, said method comprising:

a) assigning a user key to a user and storing the user key in a data processing system for encrypting messages; (see col. 2, lines 35 - 37, and col. 5, lines 55 - 57: *"Protected storage area 33 is utilized to store user public/private key pairs."*)

b) encrypting the messages with the user key; (see col. 4, lines 8 - 13: *"When an application needs to transmit an encrypted message ..... accesses the user private key ..., and then encrypts the message or signs a signature utilizing the user private key. "*)

c) storing an associated key in the data processing system and encrypting the user key with the associated key to obtain an encrypted user key; (see col. 4, lines 20 - 28: *"A random password, ..., to be associated with the user public/private key pair is then generated for the user,..... Utilizing a chip public key, the random password is first encrypted along with the user public/private key pair,")*

d) communicating encrypted messages in conjunction with the encrypted user key to validate an association of the user with the encrypted messages; (see col. 2, lines 12 - 15: *"In order to allow the signature chip to perform an authentication procedure, such as signing signatures, a user must provide a correct password to the signature chip.")*

e) thereafter, preventing validation of the association of the user with messages by revoking the associated key. (see col. 4, lines 33 - 36: *"... the user public/private key pair outside the signature chip can be discarded (by the human user) for security reasons,")*

f) computer usable media bearing said control program. (see col. 5, lines 44 - 51: " *the present invention are capable of being distributed as a program product in a variety of forms,")*

Regarding Claim 2, 10, 18, Challener discloses the method, system and program product according to Claims 1, 9, 17, further comprising:

a) decrypting the user key with the associated key; (see col. 4, lines 61 – 62: *"The signature chip decrypts the encrypted package of the first password and first symmetric key.")*

b) decrypting the messages with the user key. (see col. 2, lines 4 - 6*: "when a message is encrypted utilizing a user public key, the encrypted message may only be decrypted utilizing a user private key.")*

Regarding Claim 3, 11, 19, Challener discloses the method, system and program product according to Claim 1, 9, 17, wherein the data processing system further comprises a client system having a client memory device coupled to a server system having an encryption chip and a server memory device and wherein:

a) storing the user key in a data processing system for encrypting messages further comprises storing the *user* key in the *client* memory device; (see col. 3, lines 62 - 64: " *... user of computer system 10 has a separate and unique user public/private key pair established for each application within computer system")*

b) storing the associated key in the data processing system further comprises storing the *associated* key in the *server* memory device; (see col. 2, lines 19 - 22: *"Thus, a user private key and its respective password can only be unwrapped inside the signature chip,")*

c) preventing validation further comprises preventing the validation of the messages associated with the user by eliminating the associated key from the server memory device. (see col. 4, lines 33 – 36: *"any record of the user public/private key pair outside the signature chip can be discarded (by the human user) for security reasons,")*

Regarding Claim 4, 12, 20, Challener discloses the method, system and program product according to Claim 3, 11, 19, wherein encrypting the messages further comprises:

a) sending the messages to be encrypted from the client system to the server system; (see col. 4, lines 58 - 61: *".... the encrypted package of the first password and first symmetric key (from the hard disk) are then sent to the signature chip.")*

b) encrypting the messages using *the encryption chip* of the server system; (see col. 4, lines 47 - 49: "*Utilizing the chip public key, the first password is then encrypted along with the first symmetric key, as depicted in block 48.")*

c) sending the encrypted messages from the server system to the client system. (see col. 4, lines 49 - 51; *"The encrypted package of the first password and first symmetric key is then stored in the hard disk")*

Regarding Claim 5, 13, 21, Challener discloses the method, system and program product according to Claims 4, 12, 20, further comprising: *erasing* from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system. (see col. 4, lines 33 – 36: *"any record of the user public/private key pair outside the signature chip can be discarded (by the human user) for security reasons,")*

Regarding Claim 6, 14, 22, Challener discloses the method, system and program product according to Claim 1, 9, 17, further comprising: *encrypting* the associated key by using an encryption chip key which is stored on an encryption chip of the data processing system. (see col. 6 lines 38 - 40: *"Then, the user public/private key pair is encrypted along with a random password, utilizing a chip public key.")*

Regarding Claim 7, 15, 23, Challener discloses the method, system and program product according to Claims 6, 14, 22, further comprising:

a) encrypting the associated key with the encryption chip key; (see col. 6 lines 38 - 40: *"Then, the user public/private key pair is encrypted ..... utilizing a chip public key.")*

b) communicating an encrypted associated key to validate the association of the user with the encrypted messages. (see col. 2, lines 12 - 15: *"In order to allow the signature chip to perform an authentication procedure, such as signing signatures, a user must provide a correct password to the signature chip.")*

Regarding Claim 8, 16, 24, Challener discloses the method, system and program product according to Claims 7, 15, 23, further comprising: *decrypting* the associated key with the encryption chip key. (see col. 4, lines 61 – 62: *"The signature chip decrypts the encrypted package of the first password and first symmetric key.")*

Conclusion

Prior Art

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
   a. U.S. Patent No. 6,487,658 to Micali discloses Efficient Certificate Revocation.
   b. U.S. Patent No. 5,519,778 to Leighton discloses Method for Enabling Users of a Cryptosystem to Generate and use a Private Pair Key for Enciphering Communications between the Users.
   c. European Patent Application No. EP1185024 A2 discloses System, Method, and Program for Managing a User Key used to Sign a Message for a Data Processing System.
   d. RSA, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214273,00.html

Contact Information

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H Shin whose telephone number is 703-305-0711. The examiner can normally be reached on 6:30 am - 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS

Kyung H Shin
Patent Examiner
Art Unit 2132

KHS
March 31, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100